IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of   :

                                                    :

First Named Inventor: Vincent Carlier   : **Confirmation No.** 7126

                                                    :

U.S. Patent Application No. 10/574,909   : **Group Art Unit:** 2439

                                                    :

Filed: April 6, 2006   : **Examiner:** LAFORGIA, Christian A.

For: A METHOD OF PROTECTING A CRYPTOGRAPHIC ALGORITHM

<u>BRIEF ON APPEAL UNDER 37 C.F.R. § 41.37</u>

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

       Further to the Notice of Appeal filed August 11, 2009 in connection with the above-identified application on appeal, the Appellant respectfully submits this Brief on Appeal. Please charge any fees or credit any overpayments that may be due with this Brief to Deposit Account No. 50-3828.

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST

The real party in interest in this appeal is SAGEM DEFENSE SECURITE, Le Ponant De Paris, 27 Rue LeBlanc, 75015 Paris, France, as evidenced by the assignment recorded at Reel 017779, Frame 0679 on April 6, 2006.

II. RELATED APPEALS AND INTERFERENCES

There are no related appeals and/or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

A. Total Number of Claims in Application

There are a total of 10 claims pending in the instant application, namely claims 1-10. Claims 1 and 6 are independent claims.

B. Status of All the Claims

1. Claims cancelled: none

2. Claims withdrawn from consideration but not cancelled: none

3. Claims pending: 1-10

4. Claims allowed: none

5. Claims rejected: 1-10

C. Claims on Appeal

Claims on appeal are claims 1-10 as rejected by the Final Office Action of May 11,

2009.

IV. STATUS OF AMENDMENTS

No amendments were filed subsequent to the Final Office Action dated May 11, 2009.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 1 is directed to a method of protecting a cryptographic algorithm

(e.g., 6, FIG. 1) before introduction in an enciphering device **(e.g., 1, FIG. 1, page 2, lines 5-9)**

comprising programmable processor unit **(e.g., 4, FIG. 1)**. The algorithm being separable into

the form of initial polynomials (P_i) of at least two variables each, and having a degree of not

less than two **(e.g., page 4, lines 10-12)**. The method includes providing to the enciphering

device at least two initial polynomials (P_i, P_{i+1}) **(e.g., page 4, lines 18-20)**; combining, on the

enciphering device, combined polynomials (Q_k), each obtained from the at least two initial

polynomials (P_i, P_{i+1}) **(e.g., page 4, lines 20-22)**; and implementing the combined polynomials

(Q_k) in the programmable processor unit **(e.g., page 2, lines 17-18)**.

Dependent claim 2 is directed to a method according to claim 1, and further includes

storing the combined polynomials (Q_k) in the form of a configuration file that is loaded into a

memory **(e.g., 3, FIG. 1)** associated with the processor unit **(e.g., page 4, lines 33-34)**.

Dependent claim 3 is directed to a method according to claim 2, wherein the memory and the programmable processor unit are associated with an eraser member **(e.g., 5, FIG. 1)** serving, in the event of an intrusion into the device, to erase the processor unit, and to erase the memory containing the configuration file when the configuration is present in said memory **(e.g., page 3, line 35-page 4, line 6).**

Dependent claim 4 is directed to a method according to claim 1, which includes combining each combined polynomial (Q_k) with a function (f_k); and combining the following combined polynomial (Q_{k+1}) with an inverse function (f_k^{-1}) **(e.g., page 4, lines 25-32).**

Dependent claim 5 is directed to a method according to claim 4, wherein the function (f_k) combined with each combined polynomial (Q_k) is a linear function **(e.g., page 4, lines 25-27).**

Independent claim 6 is directed to an enciphering device **(e.g., 1, FIG. 1)** which utilizes a cryptographic algorithm **(e.g., 6, FIG. 1)**, including a programmable processor unit **(e.g., 4, FIG. 1)**; an eraser member **(e.g., 5, FIG. 1)** coupled to the programmable processor unit; and a memory **(e.g., 3, FIG. 1)** coupled to the eraser unit and the programmable processor unit **(e.g., page 3, lines 26-33)**, wherein the cryptographic algorithm is protected prior to its introduction into the enciphering device **(page 2, lines 5-9)**, and further wherein the cryptographic algorithm is separable into the form of initial polynomials (P_i) of at least two variables each, having a degree of not less than two **(e.g., page 4, lines 10-12)**, and further wherein the programmable

processor unit receives the initial polynomials (P_i, P_{i+1}) **(e.g., page 4, lines 18-20)**, and combines the at least two initial polynomials (P_i, P_{i+1}) to form combined polynomials (Q_k) **(e.g., page 4, lines 20-22)**.

Dependent claim 7 is directed to the enciphering device according to claim 6, wherein the combined polynomials (Q_k) are stored in the form of a configuration file that is loaded into the memory **(e.g., 3, FIG. 1, page 4, lines 33-34)**.

Dependent claim 8 is directed to the enciphering device according to claim 7, wherein in the event of an intrusion into the enciphering device, the eraser member **(e.g., 5, FIG. 1)** will erase the processor unit and memory containing the configuration file when the configuration is present in said memory **(e.g., page 3, line 35-page 4, line 6)**.

Dependent claim 9 is directed to the enciphering device according to claim 6, wherein each combined polynomial (Q_k) is combined with a function (f_k), and the following combined polynomial (Q_{k+1}) is combined with an inverse function (f_k^{-1}) **(e.g., page 4, lines 25-32)**.

Dependent claim 10 is directed to the enciphering device according to claim 9, wherein the function (f_k) combined with each combined polynomial (Q_k) is a linear function **(e.g., page 4, lines 25-27)**.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The Examiner has finally rejected claims 1-4 and 6-9 under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 2004/0187035 A1 ("Schwan") in view of known techniques (U.S. Patent No. 4,922,539 ("Rajasekaran"). Claims 5 and 10 are rejected under 35 U.S.C. §103(a) as being unpatentable over Schwan in view of known techniques and further in view of *Applied Cryptography, Protocols, Algorithms, and Source Code in C*, by Bruce Schneier ("Schneier ").

VII. ARGUMENT

Below, the Appellant has provided arguments related with section headers in **bold**.

A. Schwan and/or Rajasekaran fail to render claims 1-4 and 6-9 obvious under 35 U.S.C. 103(a).

Claims 1 and 6

Regarding claim 1, Appellant maintains that Schwan and Rajasekaran fail to teach or suggest, at least, "protecting a cryptographic algorithm <u>before introduction in a device</u> ... providing combined polynomials (Q_k) each obtained from at least two initial polynomials (P_i, P_{i+1}) and of implementing the combined polynomials (Q_k) in the programmable processor unit." (Emphasis added.)

Appellants maintain that Schwan does not teach or suggest protecting the algorithm **before** it is introduced in a device but when it is implemented in the device. To this effect Schwan combines two features: an encapsulation of the algorithm and a control of access to the data input (see [0007] and [0008]). Those features have nothing in common with the method of separating the algorithm into initial polynomials and combining them for safe transport.

In the Response to Arguments section on page 2 of the Final Office Action, the Examiner agrees with the Appellants that Schwan fails to show the above quoted feature.

The Examiner attempts to cure this deficiency by arguing that "the security features claimed by applicant are inherent in the known technique of factoring, specifically factoring cryptographic equation order to protect said equation prior to being implemented on a computer." (See Final Office Action, page 2, para. no. 6, lines 4-6.) The Examiner presented the Rajasekaran reference as evidence to show that "factoring was a well-known and commonly practiced technique." (See Final Office Action, page 2, para. no. 6.)

Appellants submit the above-quoted feature of claim 1 is not inherent in the technique of factoring. Moreover, the Rajasekaran reference merely teaches a form of polynomial factorization used in a speech processing context.

While polynomial factoring algorithms may be used in the field of cryptology, their use is not inherent, as the Examiner asserts, in "protecting a cryptographic algorithm before introduction in a device" as set forth in claim 1. For example, such protection of cryptographic algorithms may also be afforded using other cryptographic techniques, physical security, manufacturing protocols, etc.

For at least the aforementioned reasons, Appellant submits that claim 1 is allowable over the Schwan and Rajasekaran references.

Independent Claim 6 recites related material to claim 1 in this respect, and is also allowable at least for similar reasons.

Claims 3 and 8

Claims 3 and 8 depend from claims 1 and 6, respectfully, and are allowable at least for reasons similar to those provided above for claim 1. In addition, regarding claim 3, Schwan and Rajasekaran fail to teach or suggest "wherein an eraser member (5) serving, in the event of an intrusion into the device, to erase the processor unit." (Emphasis added.) Schwan merely teaches that "memory areas containing a secret check word and/or secret key and/or secret encryption algorithm are erased and/or destroyed so that it is no longer possible to read out said data or algorithms after the housing is opened." (See [0013], lines 2-6.) Schwan clearly describes separate memory and controller (e.g., microprocessor) components ([0002], lines 4-5), and fails to specifically teach the erasure of the controller. Moreover, Rajasekaran is completely silent with respect to this feature.

Accordingly, Appellants respectfully request that the Examiner reconsider and withdraw the rejection of claim 3. Claim 8 recites related subject matter to claim 3 in this respect, and is allowable at least for similar reasons.

Claims 2, 4, 7 and 9

Claims 2, 4, 7 and 9 depend from claims 1 and 6, respectively, and are allowable at least by virtue of their dependency.

For at least the above reasons, Appellants submit that the 35 U.S.C. § 103(a) rejection of claims 1-4 and 6-9 should now be reconsidered and withdrawn.

B.   Schwan, Rajasekaran and/or Schneier fail to render claims 5 and 10 obvious under 35 U.S.C. 103(a).

Regarding claims 5 and 10, Schneier fails to cure the deficiencies of Schwan and Rajasekaran with respect to claims 1 and 6, respectfully.   Schneier merely provides a description of DES block cipher algorithms and key transformations used therein. Accordingly, Claims 5 and 10 are therefore allowable at least by virtue of their respective dependencies from claims 1 and 6.

Accordingly, reconsideration and withdrawal of the rejections under 35 U.S.C. §103 are respectfully requested.

VIII. CLAIMS

A copy of the claims involved in the present appeal is attached hereto as Claims Appendix.

IX. EVIDENCE

No evidence pursuant to §§ 1.130, 1.131, or 1.132 or entered by or relied upon by the Examiner is being submitted.

X. RELATED PROCEEDINGS

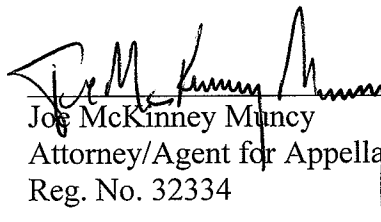No related proceedings are referenced in Section II, above.

XI. CONCLUSION

The Appellant respectfully submits that claims 1-10 are patentable over the applied art and that all of the rejections and objections of record should be reversed.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 50-3828 for any additional fees required under 37 C.F.R. §§ 1.16 or 1.17; particularly, extension of time fees.

Date: October 9, 2009   Respectfully Submitted,

Joe McKinney Muncy
Attorney/Agent for Appellants
Reg. No. 32334

Muncy, Geissler, Olds & Lowe, PLLC
PO BOX 1364
Fairfax, VA 22038-1364
Tel. 1.703.621.7140
mailroom@mg-ip.com

CLAIMS APPENDIX

1. (Previously Presented) A method of protecting a cryptographic algorithm (6) before introduction in an enciphering device (1) comprising programmable processor unit (4), the algorithm being separable into the form of initial polynomials (P_i) of at least two variables each, and having a degree of not less than two, the method comprising:

providing to the enciphering device at least two initial polynomials (P_i, P_{i+1});

combining, on the enciphering device, combined polynomials (Q_k), each obtained from the at least two initial polynomials (P_i, P_{i+1}); and

implementing the combined polynomials (Q_k) in the programmable processor unit (4).

2. (Previously Presented) A method according to claim 1, further comprising:

storing the combined polynomials (Q_k) in the form of a configuration file that is loaded into a memory (3) associated with the processor unit (4).

3. (Previously Presented) A method according to claim 2, wherein the memory (3) and the programmable processor unit (4) are associated with an eraser member (5) serving, in the event of an intrusion into the device, to erase the processor unit (4), and to erase the memory (3) containing the configuration file when the configuration is present in said memory.

4. (Previously Presented) A method according to claim 1, further comprising:

combining each combined polynomial (Q_k) with a function (f_k); and

combining the following combined polynomial (Q_{k+1}) with an inverse function (f_k^{-1}).

5. (Previously Presented) A method according to claim 4, wherein the function (f_k) combined with each combined polynomial (Q_k) is a linear function.

6. (Previously Presented) An enciphering device which utilizes a cryptographic algorithm, comprising:

a programmable processor unit;

an eraser member coupled to the programmable processor unit; and

a memory coupled to the eraser unit and the programmable processor unit, wherein the cryptographic algorithm is protected prior to its introduction into the enciphering device, and

further wherein the cryptographic algorithm is separable into the form of initial polynomials (P_i) of at least two variables each, having a degree of not less than two, and

further wherein the programmable processor unit receives the initial polynomials (P_i, P_{i+1}), and combines the at least two initial polynomials (P_i, P_{i+1}) to form combined polynomials (Q_k).

7. (Previously Presented) The enciphering device according to claim 6, wherein the combined polynomials (Q_k) are stored in the form of a configuration file that is loaded into the memory.

8. (Previously Presented) The enciphering device according to claim 7, wherein in the event of an intrusion into the enciphering device, the eraser member will erase the processor unit and memory containing the configuration file when the configuration is present in said memory.

9. (Previously Presented) The enciphering device according to claim 6, wherein each combined polynomial (Q_k) is combined with a function (f_k), and the following combined polynomial (Q_{k+1}) is combined with an inverse function (f_k^{-1}).

10. (Previously Presented) The enciphering device according to claim 9, wherein the function (f_k) combined with each combined polynomial (Q_k) is a linear function.

EVIDENCE APPENDIX

(None)

RELATED PROCEEDINGS APPENDIX

(None)